KBV

KASSENÄRZTLICHE
BUNDESVEREINIGUNG

AKTUALISIERTE
AUSGABE
2025

IT-SICHERHEIT

ANFORDERUNGEN UND SCHUTZMASSNAHMEN, TIPPS UND BEISPIELE FÜR DIE PRAXIS

DIESES THEMENHEFT ERGÄNZT
DIE ONLINE-PLATTFORM ZUR
IT-SICHERHEITSRICHTLINIE:
https://hub.kbv.de/display/itsrl

PraxisWissen

Liebe Kolleginnen, liebe Kollegen,

weltweit wächst die Bedrohung der IT-Sicherheit. Auch medizinische Einrichtungen sind das Ziel von Hacker-Angriffen, und die Bandbreite der Methoden, mit denen Kriminelle arbeiten, nimmt zu. Deshalb müssen die Schutzmaßnahmen immer wieder überprüft und angepasst werden, um unbefugte Zugriffe auf die Praxis-IT und damit auf die besonders sensiblen Patienten- und Abrechnungsdaten zu verhindern.

Bereits seit 2021 unterstützt die IT-Sicherheitsrichtlinie Sie und Ihre Praxisteams dabei, geeignete Schutzmaßnahmen zu treffen. Die Richtlinie beschreibt eine Basis-Infrastruktur für den Schutz der Praxis-IT – je nach Praxisgröße und Ausstattung. Dazu gehören zum Beispiel aktueller Virenschutz, regelhafte Updates und Backups sowie eine geeignete Netzwerksicherheit.

Die Richtlinie wurde aufgrund gesetzlicher Vorgaben erstellt und 2025 aktualisiert. Neu sind insbesondere Maßnahmen zur Sensibilisierung des Praxispersonals für Informationssicherheit. Auch enthält die Richtlinie jetzt beispielsweise die Vorgabe, den Umgang mit Spam bei E-Mails zu regeln. Alle Neuerungen müssen Praxen spätestens ab Oktober 2025 umsetzen, bisherige Anforderungen gelten weiter.

Dieses Serviceheft soll Praxisinhaberinnen und Praxisinhaber bei der Umsetzung der Richtlinie unterstützen. Das Heft erschien erstmals 2021 und wurde jetzt aktualisiert. Es stellt bekannte und neue Anforderungen vor, bietet eine Checkliste, Praxis-Tipps und Beispiele sowie weiterführende Informationen. Das Heft ist ein Serviceangebot und ergänzt den Hub zur IT-Sicherheit, wo Sie die komplette Richtlinie, sämtliche Anforderungen sowie Musterdokumente finden. Auch dazu mehr in diesem Heft.

Wir wünschen Ihnen eine angenehme Lektüre.

Ihre Kassenärztliche Bundesvereinigung

INHALT

RECHTLICHER HINWEIS: Unabhängig von der IT-Sicherheitsrichtlinie sind die rechtlichen Vorgaben beispielsweise zur ärztlichen Schweigepflicht zu beachten. Mit der IT-Sicherheitsrichtlinie wurden keine neuen Sanktionsformen eingeführt. Grundlage für Sanktionen sind wie bisher unter anderem die EU-Datenschutzgrundverordnung (z. B. bei Verstößen gegen den Datenschutz), das deutsche Strafgesetzbuch (z. B. § 203 StGB bei Verletzung von Privatgeheimnissen) und das Berufsrecht (§ 9 Abs. 1 MBO-Ärzte bei Verstößen gegen die ärztliche Schweigepflicht).

SCHUTZ DER PRAXIS-IT

Jeder Praxisinhaber und jede Praxisinhaberin möchte, dass die anvertrauten Daten sicher verwahrt sind. Mit der IT-Sicherheitsrichtlinie wurde hierfür ein verlässlicher Rahmen geschaffen. Dabei geht es um Punkte wie Sicherheitsmanagement, IT-Systeme, Rechnerprogramme, mobile Apps und Internetanwendungen oder das Aufspüren von Sicherheitsvorfällen.

GESETZLICHER AUFTRAG AN DIE KBV

Die KBV wurde vom Gesetzgeber beauftragt, in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung festzulegen. Dazu gehört auch, sie an den Stand der Technik und an das Gefährdungspotenzial anzupassen. Dies muss im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, erfolgen. Grundlage ist Paragraf 390 SGB V. Die KBV hat darauf geachtet, praktikable und realistische Vorgaben für die Praxen zu machen, die möglichst aufwandsarm umzusetzen sind.

VERLÄSSLICHER RAHMEN FÜR PRAXEN

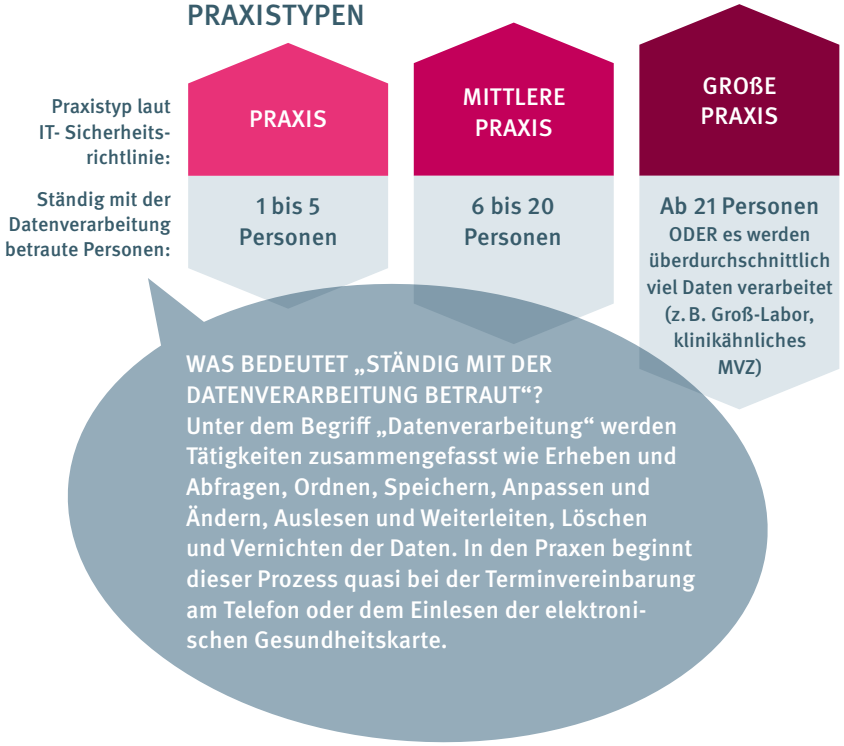
Die Richtlinie soll Praxisinhaberinnen und -inhaber dabei unterstützen, alle nötigen Sicherheitsvorkehrungen zu treffen, um einen Datenmissbrauch zu verhindern. Sie bietet ihnen damit auch ein Stück Sicherheit. Denn die Richtlinie legt Sicherheitsanforderungen an Arzt- und Psychotherapiepraxen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen. Vieles davon wird im Praxisalltag bereits angewendet, da es durch die europäische Datenschutzgrundverordnung vorgegeben ist. Neu ist, dass Praxisinhaberinnen und -inhaber ihr Personal in puncto IT-Sicherheit sensibilisieren und schulen müssen.

ANFORDERUNGEN NACH DER PRAXISGRÖßE

Die Vorgaben an die IT-Sicherheit richten sich nach der Größe der Praxis. Dabei finden sich in der Richtlinie Anforderungen, die von allen Praxen erfüllt werden müssen, um die Sicherheit der verwendeten Hard- und Software zu gewährleisten. Für Praxen, in denen mehr als fünf Personen ständig mit der Datenverarbeitung beschäftigt sind oder in denen überdurchschnittlich viele Daten verarbeitet werden (z. B. Groß-Labore), gibt es zusätzliche Anforderungen. Kommen medizinische Großgeräte zum Einsatz, zum Beispiel CT, MRT, PET, Linearbeschleuniger, sind weitere Sicherheitsvorkehrungen zu treffen. Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten sollten deshalb zunächst schauen, zu welchem Praxistyp sie gehören.

Die Anforderungen sind in den Anlagen zur Richtlinie aufgeführt.
Mehr dazu auf Seite 4.

ÜBERSICHT
PRAXISTYPEN



DAS IST FÜR PRAXEN WICHTIG

Wer in einer Arzt- oder Psychotherapiepraxis arbeitet, weiß um die sensiblen Daten, die hier erfasst und verarbeitet werden, und dass sie zu schützen sind. Doch Cyberkriminelle gehen immer raffinierter vor, und schon ein unachtsamer Klick auf den Anhang einer E-Mail kann die Praxis in Gefahr bringen.

Nachfolgend finden Sie eine Auswahl wichtiger Anforderungen aus der IT-Sicherheitsrichtlinie für Mitarbeiterinnen und Mitarbeiter sowie die Praxis-IT.

Die IT-Sicherheitsrichtlinie gibt den Rahmen vor. Entscheidend sind die Anlagen:

ANLAGE 1
Anforderungen, die alle Praxen erfüllen müssen.
Mehr dazu auf den Seiten 5 und 6.

ANLAGE 2
Anforderungen, die mittlere und große Praxen zusätzlich zu Anlage 1 erfüllen müssen.
Mehr dazu auf Seite 7.

ANLAGE 3
Anforderungen, die ausschließlich große Praxen zusätzlich zu Anlage 1 und Anlage 2 erfüllen müssen.
Mehr dazu ebenfalls auf Seite 7.

ANLAGE 4
Anforderungen, die alle Praxen zusätzlich zu Anlage 1, Anlage 2 und Anlage 3 erfüllen müssen, wenn sie medizinische Großgeräte wie CT oder MRT einsetzen.
Mehr dazu auf Seite 8.

ANLAGE 5
Anforderungen, die alle Praxen bezüglich der sogenannten dezentralen Komponenten der Telematikinfrastruktur (z. B. Konnektor, Kartenlesegerät, Praxisausweis) erfüllen müssen.
Mehr zu einigen Anforderungen auf Seite 6 sowie im Fokus auf den Seiten 12 und 13.

PRAXISPERSONAL

PFLICHT ZUR UMSETZUNG **1. OKTOBER 2025**

PRAXIS | MITTLERE PRAXIS | GROßE PRAXIS

ANFORDERUNGEN **AN ALLE PRAXEN**

› SICHERER UMGANG MIT DER IT

Alle Mitarbeiterinnen und Mitarbeiter müssen in den sicheren Umgang mit der Praxis-IT eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeit relevant ist. / Anlage 1 Nummer 9

Das gilt auch für externes Personal – siehe nächster Punkt.

› EXTERNES PERSONAL

Externe Mitarbeiterinnen und Mitarbeiter beispielsweise von Dienstleistern, die Technik installieren, prüfen oder reparieren, müssen verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Kurzfristig oder einmalig eingesetztes externes Personal muss in sicherheitsrelevanten Bereichen beaufsichtigt werden. Zugangsberichtigungen sind so restriktiv wie möglich zu halten. / Anlage 1 Nummer 3

Bevor eine externe Person Zugang zu vertraulichen Informationen erhält oder darauf zugreifen kann, muss eine Vertraulichkeitsvereinbarung in schriftlicher Form geschlossen werden. / Anlage 1 Nummer 4

Info: Hierzu finden Sie im Hub ein Musterdokument: „Muster-Verschwiegenheitserklärung (extern)“.

› TECHNISCH VERSIERTER UMGANG

Das Praxispersonal muss angemessen qualifiziert sein und regelmäßig geschult beziehungsweise weitergebildet werden, insbesondere bezüglich der eingesetzten Technik/IT. / Anlage 1 Nummer 6

› SCHULUNG ZUR INFORMATIONSSICHERHEIT

Die Mitarbeiterinnen und Mitarbeiter sollten entsprechend ihrer Aufgaben und Verantwortlichkeiten zu Themen der Informationssicherheit geschult werden. / Anlage 1 Nummer 10

Info: Näheres zu Schulungen finden Sie im Hub zur IT-Sicherheit unter „Fortbildungen“.

› SENSIBILISIERUNG DER PRAXISLEITUNG

Gibt es in der Praxis eine Praxisleitung, so muss der Praxisinhaber oder die Praxisinhaberin diese ausreichend für Sicherheitsfragen sensibilisieren. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden. / Anlage 1 Nummer 8

› UMGANG MIT SPAM BEI E-MAILS

In der Praxis sollte der Umgang mit Spam bei E-Mails geregelt sein. Grundsätzlich sollten alle Mitarbeiterinnen und Mitarbeiter Spam-E-Mails ignorieren und löschen. Sie sollten auf unerwünschte E-Mails nicht antworten und Links in diesen E-Mails nicht folgen. / Anlage 1 Nummer 41

› VERSCHWIEGENHEIT

Alle Mitarbeiterinnen und Mitarbeiter müssen verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Sie sind darauf hinzuweisen, dass während der Arbeit erhaltene Informationen nur für den internen Gebrauch sind. / Anlage 1 Nummer 5

Info: Hierzu finden Sie im Hub ein Musterdokument: „Muster-Verschwiegenheitserklärung (intern)“.

› VERTRAUENSWÜRDIGES PERSONAL

Beim Einstellen neuer Mitarbeiterinnen und Mitarbeiter sollte besonders darauf geachtet werden, dass diese vertrauenswürdig sind. Dazu gehört die Prüfung der Arbeitszeugnisse und der Angaben, die relevant für die Einschätzung der Vertrauenswürdigkeit sind. / Anlage 1 Nummer 7

› EINARBEITUNG NEUER KOLLEGINNEN UND KOLLEGEN

Neues Praxispersonal muss zu Beginn der Beschäftigung in die Praxis-IT eingearbeitet und über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden. / Anlage 1 Nummer 1

Info: Hierzu gibt es im Hub ein Musterdokument: „Muster-Eintrittsformular“.

› REGELUNGEN FÜR DEN AUSTRITT

Gehen Mitarbeiterinnen und Mitarbeiter beispielsweise in Rente oder kündigen, müssen sie Arbeitsunterlagen, Schlüssel, Geräte, Ausweise und Zutrittsberechtigungen zurückgeben. Die Praxisleitung muss bekannte oder verwendete Passwörter und andere Zugangsdaten ändern oder vernichten. / Anlage 1 Nummer 2

Info: Auch zum Austritt ist im Hub ein Musterdokument abrufbar: „Muster-Austrittsformular“.

↗ Verantwortlich für die IT-Sicherheit der eigenen Praxis ist stets der Inhaber oder die Inhaberin. Sie können sich von IT-Dienstleistern unterstützen lassen. Als optionales Angebot bietet die KBV ein Verzeichnis mit IT-Dienstleistern, die speziell für die Umsetzung der IT-Sicherheitsrichtlinie zertifiziert wurden: ***https://www.kbv.de/426551***

PRAXIS-IT

PFLICHT ZUR UMSETZUNG SEIT 2021

PRAXIS | MITTLERE PRAXIS | GROßE PRAXIS

ANFORDERUNGEN **AN ALLE PRAXEN**

› SICHERE APPS NUTZEN
Apps sollten nur aus den offiziellen Stores geladen werden. Werden Apps nicht mehr benötigt, ist der Benutzeraccount in der App/das Benutzerkonto zu löschen und die App mit allen enthaltenen Daten auf dem Gerät zu deinstallieren. / Anlage 1 Nummer 42

› DATENABFLUSS VERHINDERN
Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden. / Anlage 1 Nummer 44

› KRYPTOGRAFISCHE SICHERUNG VERTRAULICHER DATEN
Bei der Nutzung von Webanwendungen ist darauf zu achten, dass eine verschlüsselte Kommunikation zum Einsatz kommt (z. B. https statt http). / Anlage 1 Nummer 49

› ABMELDEN ODER SPERREN
Nach der Nutzung eines Gerätes meldet sich die Person ab oder sperrt es. / Anlage 1 Nummer 19

› VIRENSCHUTZ-PROGRAMME
In der Praxis werden aktuelle Virenschutzprogramme eingesetzt. / Anlage 1 Nummer 20

› ZUGRIFFSSCHUTZ VERWENDEN
Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt. / Anlage 1 Nummer 32

› DOKUMENTATION DES NETZES
Das interne Netzwerk ist anhand eines Netzplanes dokumentiert. / Anlage 1 Nummer 12

Info: Einen Muster-Netzplan finden Sie im Hub.

› KEINE UNAUTORISIERTE NUTZUNG VON RECHNER-MIKROFONEN UND KAMERAS
Kamera und Mikro sollten grundsätzlich deaktiviert sein und nur bei Bedarf aktiviert und danach wieder deaktiviert werden. / Anlage 1 Nummer 18

› SICHERE SPEICHERUNG LOKALER APP-DATEN
Es werden nur Apps genutzt, die Dokumente verschlüsselt und lokal abspeichern. / Anlage 1 Nummer 43

› WEB APPLICATION FIREWALL (WAF)
Wenn Sie als Praxis einen Webdienst anbieten, dann sollten Sie eine Web Application Firewall (WAF) einsetzen. Die Konfiguration der eingesetzten WAF sollte auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices sollte die Konfiguration der WAF geprüft werden. / Anlage 1 Nummer 47

› SCHUTZ VOR UNERLAUBTER AUTOMATISIERTER NUTZUNG VON WEBANWENDUNGEN
Wenn Sie als Praxis einen Webdienst anbieten, dann muss Ihre Praxis sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei muss jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, muss dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden. / Anlage 1 Nummer 48

› REGELMÄßIGE DATENSICHERUNG
Auf Endgeräten, zum Beispiel einem Praxisrechner, erfolgt eine regelmäßige Datensicherung, wobei in einem Plan festgelegt ist, welche Daten wie oft gesichert werden sollen. / Anlage 1 Nummer 21

› SPERRMAßNAHMEN BEI VERLUST EINES MOBILTELEFONS
Bei Verlust eines Mobiltelefons (Diensthandy) muss die darin verwendete SIM-Karte zeitnah gesperrt werden. / Anlage 1 Nummer 34

› SCHUTZ VOR SCHADSOFTWARE
Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden. / Anlage 1 Nummer 36

› ZEITNAHES INSTALLIEREN VERFÜGBARER AKTUALISIERUNGEN
Für die dezentralen Komponenten der Telematikinfrastruktur werden Updates zeitnah installiert. / Anlage 5 Nummer 8

› SICHERES AUFBEWAHREN VON ADMINISTRATIONSDATEN
Für die dezentralen Komponenten der Telematikinfrastruktur werden die Administrationsdaten sicher aufbewahrt. Jedoch muss gewährleistet sein, dass Sie als Praxisinhaberin bzw. Praxisinhaber auch ohne Ihren Dienstleister die Daten kennen. / Anlage 5 Nummer 9

PFLICHT ZUR UMSETZUNG
1. OKTOBER 2025:

› INSTALLATION VON UPDATES
Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden. / Anlage 1 Nummer 14

MITTLERE PRAXIS GROßE PRAXIS

ZUSÄTZLICHE ANFORDERUNGEN AN MITTLERE UND GROßE PRAXEN

› MINIMIERUNG UND KONTROLLE VON APP-BERECHTIGUNGEN

Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken. / Anlage 2 Nummer 10

› REGELUNGEN FÜR DIE MOBILTELEFON-NUTZUNG

Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden. / Anlage 2 Nummer 7

Info: Nutzen Sie dazu die Muster-Richtlinie mobile Geräte im Hub.

› RICHTLINIE ZUR NUTZUNG VON MOBILEN GERÄTEN

Werden Smartphones und Tablets genutzt, sollte es dazu eine verbindliche Richtlinie geben. / Anlage 2 Nummer 5

Info: Nutzen Sie dazu ebenfalls die Muster-Richtlinie mobile Geräte im Hub.

› REGELUNG ZUR MITNAHME VON WECHSELDATENTRÄGERN

Werden Wechseldatenträger eingesetzt, sollte es eine Regelung zur Mitnahme geben. / Anlage 2 Nummer 9

Info: Nutzen Sie dazu die Muster-Richtlinie Wechseldatenträger im Hub.

GROßE PRAXIS

ZUSÄTZLICHE ANFORDERUNGEN AN GROßE PRAXEN

› RICHTLINIE FÜR SMARTPHONES UND TABLETS

Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. / Anlage 3 Nummer 4

Info: Nutzen Sie dazu die Muster-Richtlinie mobile Geräte im Hub.

› AUSWAHL UND FREIGABE VON APPS

Bevor Apps genutzt werden, sollten sie geprüft und freigegeben werden. / Anlage 3 Nummer 5

↗ Die jeweiligen Anforderungen müssen erfüllt werden, wenn die Praxis entsprechende IT-Komponenten verwendet.

PRAXIS | MITTLERE PRAXIS | GROSSE PRAXIS

ZUSÄTZLICHE ANFORDERUNGEN AN ALLE PRAXEN MIT MEDIZINISCHEN GROSSGERÄTEN

› ZUGRIFF EINSCHRÄNKEN FÜR FÜR KONFIGURATIONS- UND WARTUNGSSCHNITTSTELLEN

Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiterinnen und Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können.
/ Anlage 4 Nummer 1

› SICHERE PROTOKOLLE FÜR DIE KONFIGURATION UND WARTUNG

Für die Konfiguration und Wartung von medizinischen Großgeräten müssen sichere Protokolle genutzt werden.
/ Anlage 4 Nummer 2

› NETZSEGMENTIERUNG

Medizinische Großgeräte sollten von der weiteren IT getrennt sein.
/ Anlage 4 Nummer 6

Info: Medizinische Großgeräte sind beispielsweise CT, MRT, PET, Linearbechleuniger.

↗ Alle Anforderungen sowie Musterdokumente, die jede Praxis für sich anpassen kann, stehen im Hub bereit: ***https://hub.kbv.de/display/itsrl***

Mehr dazu auf Seite 14 in diesem Serviceheft.

DARAUF ACHTET DIE KBV

Bei der IT-Sicherheitsrichtlinie achtet die KBV darauf, praktikable und realistische Vorgaben für die Praxen zu machen, die möglichst aufwandsarm umzusetzen sind. Vieles wird im Praxisalltag bereits angewendet, weil es beispielsweise durch die EU-Datenschutzgrundverordnung vorgegeben ist.

Es geht um sensible Gesundheitsdaten, die besonders geschützt werden müssen. Praxisinhaberinnen und Praxisinhaber tragen hierfür eine hohe Verantwortung. Die Richtlinie soll sie dabei unterstützen und ihnen einen verlässlichen Handlungsrahmen bieten.

Im Gesetz ist auch festgelegt, dass der Umfang der Richtlinie jährlich überprüft werden muss. Das ist ein guter Weg, jeweils auf Veränderungen im IT-Bereich und Sicherheitsfragen zu reagieren. Die KBV wird darauf achten, dass auch bei den Anpassungen immer die Praktikabilität im Vordergrund steht.

CHECKLISTE
SO KÖNNEN SIE VORGEHEN

Sie wollen prüfen, ob Sie die Anforderungen der IT-Sicherheitsrichtlinie erfüllen oder welche Maßnahmen Sie zusätzlich ergreifen müssen, um vertrauliche Daten noch besser vor unberechtigten Zugriffen zu schützen? Doch womit fangen Sie am besten an? Die Checkliste soll Ihnen helfen, einen Einstieg zu finden.

1 PRAXISTYP FESTLEGEN

Welcher Praxistyp sind wir?
Je nach Praxistyp müssen die Anforderungen nach den entsprechenden Anlagen erfüllt werden:

Praxis mit 1 bis 5 Personen*
Anlage 1, 5 (und 4 bei medizinischen Großgeräten)

Mittlere Praxis mit 6 bis 20 Personen*
Anlage 1, 2, 5 (und 4 bei medizinischen Großgeräten)

Große Praxis ab 21 Personen*
oder mit Verarbeitung überdurchschnittlich vieler Daten
Anlage 1, 2, 3, 5 (und 4 bei medizinischen Großgeräten)

* ständig mit der Datenverarbeitung betraute Personen

2 IT-KOMPONENTEN FINDEN

Welche IT-Komponenten nutzen wir in unserer Praxis?
Erstellen Sie eine Liste der IT-Komponenten. Nur wenn eine IT-Komponente vorhanden ist, müssen Sie die Anforderungen erfüllen und Sicherungsmaßnahmen umsetzen.

Dezentrale Komponenten der TI, zum Beispiel Konnektor, Kartenlesegerät, Praxisausweis

Endgeräte, zum Beispiel Computer, Laptop, Notebook

Endgeräte mit Windows-Betriebssystem,
zum Beispiel Computer, auf denen Windows läuft

Internet-Anwendungen, zum Beispiel praxisbetriebene Webpräsenz, selbst betriebene Onlineterminvergabe

Medizinische Großgeräte, zum Beispiel CT, MRT, PET

Mobile Anwendungen (Apps)

Mobile Device Management / MDM,
zum Beispiel mobile Geräte wie Praxis-Laptops oder Praxis-Tablets werden zentralisiert überwacht/verwaltet

Netzwerksicherheit, zum Beispiel (W)LAN-Sicherheit

Office-Produkte, zum Beispiel Programme für Textverarbeitung, Tabellenkalkulation, Präsentationen

Dienstlich genutzte Mobiltelefone, Smartphones und Tablets

Wechseldatenträger, Speichermedien, zum Beispiel USB-Sticks, Speicherkarten, externe Festplatten

↗ Die IT-Komponenten sind im Hub in den Anlagen unter „Zielobjekt“ aufgeführt: ***https://hub.kbv.de/display/itsrl***

3 PRAXISPERSONAL EINBINDEN UND MAßNAHMEN FESTLEGEN

Wie schützen wir die IT-Komponenten unserer Praxis?
Sensibilisieren Sie Ihr Praxisteam für Informationssicherheit (Stichwort Security Awarness) und binden Sie Ihre Mitarbeiterinnen und Mitarbeiter je nach Bedarf, Aufgabe und Verantwortlichkeit bei den Sicherheitsmaßnahmen ein. Nutzen Sie Schulungsmaterial und fragen Sie hierzu bei Ihrer Kassenärztlichen Vereinigung nach.
TIPP: Die KBV wird Schulungsmaterial bereitstellen – mehr dazu im Hub zur IT-Sicherheit.

↗ Informationen, Fragen und Antworten sowie Musterdokumente finden Sie im Hub: ***https://hub.kbv.de/display/itsrl***

4 DIENSTLEISTER JA ODER NEIN?

Beauftragen wir einen IT-Dienstleister, der uns berät und unterstützt?
Die KBV veröffentlicht eine Liste der IT-Dienstleister, die speziell für die Umsetzung der Vorgaben aus der IT-Sicherheitsrichtlinie zertifiziert wurden. Dies ist ein optionales Angebot. Praxisinhaberinnen und -inhaber können sich auch für einen nicht zertifizierten Dienstleister entscheiden, wenn sie sich Hilfe holen möchten.

↗ Die Liste der IT-Dienstleister steht online zur Verfügung: ***https://www.kbv.de/426551***

5 UMSETZUNG STARTEN

Beginnen Sie mit der Umsetzung und tauschen Sie sich dazu gegebenenfalls mit Ihrem IT-Dienstleister aus.
Berücksichtigen Sie das Thema IT-Sicherheit regelmäßig in Ihren Teambesprechungen.

PRAXIS-TIPPS ZUR IT-SICHERHEIT

Nach dem Überblick auf den Seiten 4 bis 8 stellen wir hier beispielhaft einige Anforderungen näher vor. Tipps und Hinweise sollen Sie bei der Umsetzung unterstützen. Die Regelungen müssen von allen Praxen erfüllt werden, sofern die entsprechenden IT-Komponenten verwendet werden. Fachbegriffe wie Firewall oder Ports und Bezeichnungen wie „vertrauliche Daten“ werden kurz erläutert.

RECHTLICHER HINWEIS: Diese Übersicht ist keine Rechtsquelle. Die rechtlich verbindlichen Anforderungen stehen in der IT-Sicherheitsrichtlinie mit ihren Anlagen. Diese ist im Hub abrufbar. Auf dieser extra eingerichteten Plattform sind alle Anforderungen aufgeführt und mit Erläuterungen, Hinweisen und Begleitinformationen versehen. Dort finden Sie auch Musterdokumente: ***https://hub.kbv.de/display/itsrl***

PRAXISCOMPUTER

Ihre Praxis setzt aktuelle Virenschutzprogramme ein.
Anlage 1 Nummer 20

TIPP

↗ Verwenden Sie „Windows Defender“ oder ein anderes kommerzielles Virenschutzprogramm.
↗ Legen Sie fest, welche Daten wann gescannt werden sollen, zum Beispiel jede eingehende E-Mail.

HINWEIS: *Ein Virenschutz- oder Antivirenprogramm ist eine Software, die Computerviren, aber beispielsweise auch sogenannte Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll.*

Jede Person, die in Ihrer Praxis Daten verarbeitet, muss sich nach der Nutzung eines Gerätes abmelden oder das Gerät sperren.
Anlage 1 Nummer 19

TIPP

↗ Es gibt Tastenkombinationen, zum Beispiel „Windows“ + „L“ für die Sperrung bei Windows.
↗ Weisen Sie Ihr Team auf die Abmeldung hin, beispielsweise durch einen Hinweis auf einem Zettel.

UPDATES

Sie installieren Updates zeitnah nach deren Veröffentlichung.
Anlage 1 Nummer 14

TIPP

↗ Achten Sie auf Updates. PVS-Updates erfolgen in der Regel bei einem Quartalswechsel, Sicherheitsupdates können aber auch unregelmäßig erfolgen, gegebenenfalls also häufiger.

PRAXISNETZWERK

Ihr internes Netzwerk ist anhand eines Netzplanes dokumentiert.
Anlage 1 Nummer 12

TIPP

↗ Nutzen Sie das Musterdokument im Hub zur IT-Sicherheitsrichtlinie.
↗ Dokumentieren Sie die logische Struktur des Netzes, insbesondere seine Teile und Teilstrukturen (Subnetze).
↗ Dokumentieren Sie Änderungen im Netzwerk mit Datum.

HINWEIS: *Ein Netzwerk ist die Infrastruktur der von Ihnen verwendeten Hard- und Software sowie der jeweiligen Verbindungen. Ähnlich einem Stromnetz kann es schematisch als Netzplan dargestellt werden.*

Sie schützen den Übergang zu anderen Netzen, zum Beispiel das Internet, durch eine Firewall.
Anlage 1 Nummer 11

TIPP

↗ Stellen Sie die Firewall so ein, dass nur erlaubte IP-Adressen, Ports (ein- und ausgehend) und Kommunikationsprotokolle zugelassen werden.

HINWEIS: *Eine Firewall ist ein Programm, das Computer oder Netzwerke vor unerwünschten Zugriffen schützen soll. Eine IP-Adresse macht in einem Netzwerk die daran angeschlossenen Geräte erreichbar (adressierbar). Ports sind während einer Verbindung die jeweiligen Endstellen. Kommunikationsprotokolle bilden eine Grundlage für die Vernetzung. Die Datenübertragung zwischen mehreren Parteien wird hier definiert, also wie die Kommunikation erfolgt.*

WECHSELDATENTRÄGER / SPEICHERMEDIEN

Wenn Sie Wechseldatenträger oder Speichermedien versenden, tun Sie dies mit einer sicheren Versandart und Verpackung. Anlage 1 Nummer 38

TIPP

↗ Informieren Sie sich bei Ihrem Versanddienstleister über sichere Nachweissysteme wie Einschreiben und Wertsendungen.

MOBILE ANWENDUNGEN (APPS)

In Ihrer Praxis werden Apps nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.
Anlage 1 Nummer 42

TIPP

↗ Verwenden Sie für IOS „App Store“ und für Android „Google Play“.
↗ Lassen Sie in den Sicherheitseinstellungen keine Apps aus externen Quellen zu.

HINWEIS: *Apps gibt es für etliche Anwendungen, zum Beispiel um Text-, Sprach- und Bildnachrichten auszutauschen. Zu finden sind die mobilen Anwendungen in App-Stores, den digitalen Vertriebsplattformen. Offizielle App-Stores sind beispielsweise der App Store von Apple oder der Google Play Store.*

In Ihrer Praxis wird ein sogenannter Datenabfluss verhindert.
Anlage 1 Nummer 44

TIPP

↗ Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.
↗ Kommunizieren Sie dieses Vorgehen in Ihrem Team.
↗ Schränken Sie den Datenversand ein, um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden.
↗ Überprüfen Sie vor der App-Benutzung, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten.

HINWEIS: *Vertrauliche Daten sind zum Beispiel Patientenbefunde und andere personenbezogene Daten, die nicht für die Öffentlichkeit bestimmt sind und deren Verlust oder Veröffentlichung zu einem Nachteil oder Schaden führen kann.*

MOBILTELEFONE, SMARTPHONES UND TABLETS

Die Mobiltelefone, Smartphones und Tablets Ihrer Praxis sind mit einem komplexen Gerätesperrcode geschützt.
Anlage 1 Nummer 32

TIPP

↗ Verwenden Sie keine einfachen Codes, die beispielsweise nur aus vier Zahlen bestehen. Wählen Sie komplexe, lange Codes (zum Beispiel insgesamt zwölf Zeichen), die aus einer Kombination von Ziffern und Buchstaben in Groß- und Kleinschreibung bestehen. Damit wird verhindert oder zumindest erschwert, einen Code zu knacken.
↗ Setzen Sie nicht denselben Code für alle Geräte ein.

INTERNET-ANWENDUNG

In Ihrer Praxis werden verschlüsselte Internet-Anwendungen genutzt.
Anlage 1 Nummer 49

TIPP

↗ Achten Sie auf Internetseiten, die mit „https://“ beginnen. https steht für hypertext transfer protocol secure und ist ein sicheres Hypertext-Übertragungsprotokoll, mit dem Daten verschlüsselt übertragen werden können.
↗ Achten Sie auf ein Schloss, das als Icon im Webbrowser angezeigt ist. Durch Anklicken des Schlosses lassen sich Informationen zum Zertifikat und Herausgeber einsehen.

HINWEIS: *Verschlüsselung bedeutet, dass eine Klarschrift in eine Geheimschrift umgewandelt wurde und nur mit dem richtigen Schlüssel zurückverwandelt werden kann.*

TELEMATIKINFRASTRUKTUR: ANFORDERUNGEN AN DEZENTRALE KOMPONENTEN

Die Telematikinfrastruktur, kurz TI, vernetzt Akteure im Gesundheitswesen und ermöglicht eine schnelle und sichere Kommunikation zwischen ihnen. Dabei gelten für alle Komponenten – unabhängig von der IT-Sicherheitsrichtlinie – hohe Anforderungen an die Funktionalität und Sicherheit. So dürfen zum Beispiel nur Konnektoren und Kartenterminals genutzt werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert und von der gematik, der Betreibergesellschaft der TI, zugelassen sind.

UNTERSCHEIDUNG ZENTRALE UND DEZENTRALE KOMPONENTEN

Die Komponenten der zentralen TI-Plattform werden im Auftrag der gematik in Rechenzentren betrieben, sodass hier die gematik für deren Sicherheit zuständig ist. Dagegen werden die dezentralen Komponenten der TI-Plattform in den Praxen betrieben. Auf diese Komponenten bezieht sich die IT-Sicherheitsrichtlinie. Die Anforderungen sind in Anlage 5 der IT-Sicherheitsrichtlinie enthalten. Sie müssen von allen Praxen erfüllt werden (siehe auch Seite 6 in diesem Heft).

Dezentrale Komponenten sind insbesondere:

- Konnektoren
- Kartenlesegeräte
- Praxisausweise (SMB-C Karte)
- elektronische Heilberufsausweise (eHBA)

↗ Näheres zu den Komponenten finden Sie auf der Themenseite Telematikinfrastruktur: ***https://www.kbv.de/582539***

DREI BEISPIELE

BEISPIEL 1

UPDATES MÜSSEN ZEITNAH INSTALLIERT WERDEN

Automatische Updates könnten dazu führen, dass der laufende Praxisbetrieb mitten in einer medizinischen Behandlung unterbrochen wird. Daher wird bei der TI das Vorhandensein neuer Updates, beispielsweise für den Konnektor, nur angezeigt, diese werden aber nicht automatisch installiert. In der IT-Sicherheitsrichtlinie ist für alle Praxen ein „zeitnahes Installieren verfügbarer Aktualisierungen“ vorgegeben (Anlage 5 Nummer 8). Praxisinhaber müssen somit ein Update aufspielen, sie können aber selbst bestimmen, dass dies zum Beispiel nicht um 12 Uhr mittags, sondern um 2 Uhr nachts erfolgt. Updates sind für die Sicherheit und Funktionalität erforderlich.

BEISPIEL 2

ADMINISTRATIONSDATEN MÜSSEN SICHER AUFBEWAHRT WERDEN

Die bei der Installation der TI-Komponenten eingerichteten Administrationsdaten müssen sicher aufbewahrt werden (Anlage 5 Nummer 9). Das sind insbesondere Passwörter für den Administrator-Zugang des Konnektors. Jedoch muss gewährleistet sein, dass Praxisinhaber auch ohne den IT-Dienstleister Zugriff auf die Daten haben. Sie können die Administrationsdaten beispielsweise in einem versiegelten Umschlag an einem sicheren Ort hinterlegen. Sollte ein Dienstleister sich weigern, die Daten herauszugeben, so sollte zumindest mit ihm vereinbart werden, dass er die Zugangsdaten zum Vertragsende herausgibt.

BEISPIEL 3

SICHERHEITSANFORDERUNGEN GELTEN ÜBER DEN GANZEN LEBENSZYKLUS DER IT-KOMPONENTEN (UND DARÜBER HINAUS)

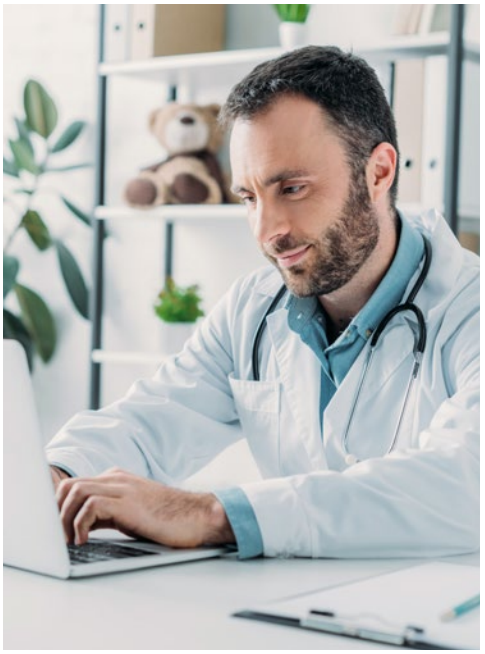
Der Chaos Computer Club (CCC) hat Ende 2024 dargelegt, dass er mit gebraucht gekauften TI-Komponenten (Konnektor, E-Health-Kartenterminal und Praxisausweis in Form der SMC-B-Chipkarte inklusive erfragter PIN) theoretisch Zugang zur Telematikinfrastruktur und damit auch zur elektronischen Patientenakte erlangt hätte.

Der Verkauf dieser Komponenten, zum Beispiel bei einer Praxisabgabe, ist besonders kritisch, da Unberechtigte darüber Zugang zu Patientendaten erlangen könnten. Die gematik stellt Informationen bereit, wie Konnektoren und Kartenterminals außer Betrieb genommen werden sollen. Dazu gehört unter anderem die Deregistrierung und Zurückstellung auf die Werkseinstellung der Konnektoren und die Entnahme der Gerätekarte (gSMC-KT) und das Löschen der Pairing-Informationen im E-Health-Kartenterminal.

Die SMC-B-Chipkarte und die gerätespezifische Chipkarte des E-Health-Kartenterminals (gSMC-KT) sollten nicht weiterverkauft werden, und die dazugehörigen PINs sollten Unberechtigten nicht offenbart werden.

↗ Mehr Informationen zur richtigen Entsorgung: ***https://www.gematik.de/newsroom/news-detail/aktuelles-konnektoren-und-e-health-kartenterminals-richtig-entsorgen***

DER HUB ZUR IT-SICHERHEIT



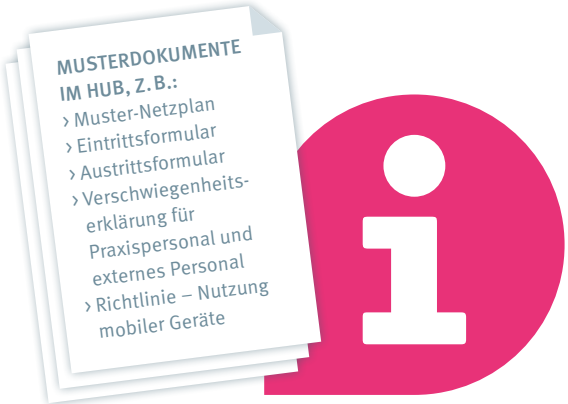
Sie wollen sich detailliert zu den einzelnen Sicherheitsanforderungen informieren, suchen Musterdokumente oder wollen eine Frage stellen? Dann nutzen Sie den Hub der KBV.

Die Online-Plattform wurde speziell zur IT-Sicherheitsrichtlinie eingerichtet und bündelt alle Informationen. Dort finden Sie die Richtlinie mit ihren Anlagen. Jede Anlage ist als Tabelle aufgebaut und besteht aus diesen Spalten:

- Nummer der Anforderung
- Zielobjekt
- Anforderung
- Erläuterung

Eine weitere Spalte enthält Hinweise wie Sie, beziehungsweise der von Ihnen beauftragte IT-Dienstleister, die Anforderungen umsetzen können.

Außerdem können Sie im Hub Musterdokumente für Ihre Praxis herunterladen, zum Beispiel einen Muster-Netzplan und eine Muster-Richtlinie für Mitarbeitende zur Nutzung von mobilen Geräten.



↗ Der Hub zur IT-Sicherheit:
https://hub.kbv.de/display/itsrl

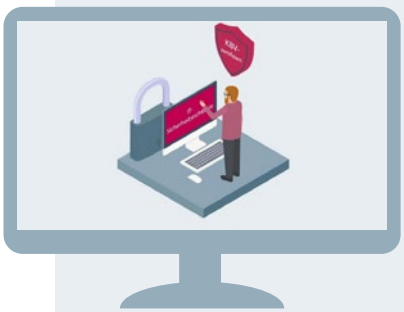
WEITERE SERVICEANGEBOTE
THEMENSEITE DER KBV ZUR IT-SICHERHEITSRICHTLINIE

Dort sind alle Informationen und Serviceangebote abrufbar beziehungsweise es wird darauf verlinkt. Dazu gehört etwa die IT-Notfallkarte „Verhalten bei IT-Notfällen“, die vom BSI angeboten wird.

Abrufbar ist auf der Themenseite auch die PraxisInfo: „IT-Sicherheit – Praxen im Visier von Hackern und Trojanern. Beispiele und Tipps zur Prävention“.

Das Video „IT-Sicherheitsrichtlinie im Überblick“ bietet einen anschaulichen Einstieg ins Thema. In wenigen Minuten wird erläutert, warum die IT-Sicherheitsrichtlinie wichtig ist und was dazu gehört.

↗ Themenseite:
https://www.kbv.de/426551



SICHERE KOMMUNIKATION MIT KIM

Arztbriefe, Befunde oder AU-Bescheinigungen so einfach versenden wie eine E-Mail: Mit einem Dienst für sichere Kommunikation im Medizinwesen (KIM) geht das. Nutzer sind Praxen, Krankenhäuser, Apotheken etc. – alle, die an die Telematikinfrastruktur (TI) angeschlossen sind.

Ein Anbieter ist die KBV. Ihr KIM-Dienst kv.dox wurde im Dezember 2020 von der gematik zugelassen und kann seitdem bestellt werden. Ärzte und Psychotherapeuten können darüber mit allen KIM-Nutzern Daten austauschen. Das Besondere: Anders als bei einem herkömmlichen E-Mail-Programm sind sensible Patienten- und Arztdaten sicher und zuverlässig geschützt. Denn der Ende-zu-Ende verschlüsselte Kommunikationsdienst ist Teil der TI.

↗ Erste Schritte, Bestellhinweise und weitere Informationen: ***https://kbv.de/kv.dox***

MEHR FÜR IHRE PRAXIS

www.kbv.de

PraxisWissen
PraxisWissenSpezial
Themenhefte für Ihren Praxisalltag

Abrufbar und kostenfrei bestellbar unter:
www.kbv.de/838223

PraxisInfo
PraxisInfoSpezial
Themenpapiere mit Informationen für Ihre Praxis

Abrufbar unter:
www.kbv.de/605808

PraxisNachrichten
Der wöchentliche Newsletter per E-Mail oder App

Abonnieren unter:
www.kbv.de/PraxisNachrichten
www.kbv.de/kbv2go

IMPRESSUM

Herausgeberin: Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
Telefon 030 4005-0, info@kbv.de, www.kbv.de
Redaktion: Bereich Interne Kommunikation im Stabsbereich Strategie, Politik und Kommunikation
Fachliche Begleitung: Dezernat Digitalisierung und IT
Gestaltung: büro lüdke GmbH
Fotos: © AdobeStock: contrastwerkstatt (S. 13), H_Ko (S. 13), Krakenimages (S. 13), Lightfield Studios (S. 14), Robert Kneschke (S. 7), Sharne T/peopleimages (S. 15), Suteren Studio(S. 4), tippapatt (S. 10); © Fotolia: Engine Images (S. 8); © gettyimages: Tetra Images (S.1); © KBV (S. 14)
Stand: Mai 2025

Aus Gründen der Lesbarkeit wurde mitunter nur eine Form der Personenbezeichnung gewählt. Hiermit sind selbstverständlich auch alle anderen Formen gemeint.